

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-005644

(43)Date of publication of application : 08.01.2003

(51)Int.Cl.

G09C 1/00

(21)Application number : 2002-089675

(71)Applicant : MATSUSHITA ELECTRIC IND CO  
LTD

(22)Date of filing : 27.03.2002

(72)Inventor : FUDA YUICHI  
ONO TAKATOSHI  
OMORI MOTOJI

(30)Priority

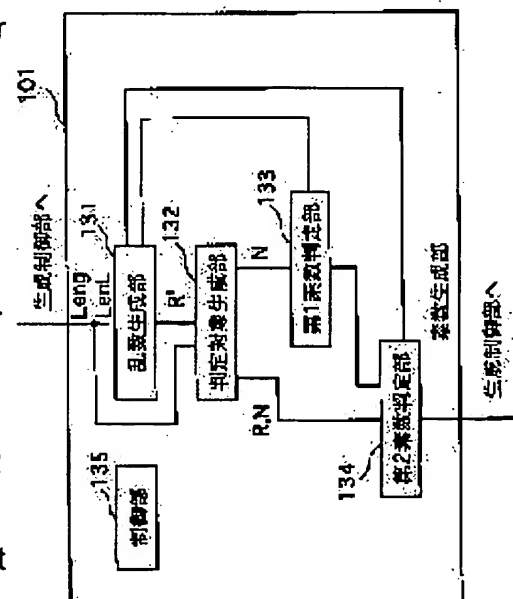
Priority number : 2001117842 Priority date : 17.04.2001 Priority country : JP

## (54) INFORMATION SECURITY APPARATUS, APPARATUS AND METHOD FOR GENERATING PRIME NUMBER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a prime number generating apparatus which can reduce a quantity of calculation and definitely generate prime numbers.

SOLUTION: An information security apparatus inputs a prime number  $q$  and generates a prime number  $N$  greater than  $q$  and is provided with a partial information setting part, a random number generating part, a part for generating an object to be determined and a part for determining the prime number. The partial information setting part generates the number  $u$  meeting a formula  $2 \times u \times q + 1 \neq 0 \pmod{L_i}$  ( $i=1, 2, \dots, n$ ). The random number generating part generates a random number  $R'$ . The part for generating the object to be determined generates  $R = u + L_1 \times L_2 \times \dots \times L_n \times R'$  and  $N = 2 \times R \times q + 1$  by using the number  $u$  and the random number  $R'$ . The part for determining the prime number determines the prime number by using the numbers  $N$  and  $R$ .



---

**LEGAL STATUS**

[Date of request for examination] 13.12.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-5644

(P2003-5644A)

(43) 公開日 平成15年1月8日 (2003.1.8)

(51) Int.Cl.<sup>7</sup>

G 0 9 C 1/00

識別記号

6 5 0

6 6 0

F I

G 0 9 C 1/00

テマコード (参考)

6 5 0 Z 5 J 1 0 4

6 6 0 A

審査請求 未請求 請求項の数12 O L (全 20 頁)

(21) 出願番号 特願2002-89675 (P2002-89675)  
(22) 出願日 平成14年3月27日 (2002.3.27)  
(31) 優先権主張番号 特願2001-117842 (P2001-117842)  
(32) 優先日 平成13年4月17日 (2001.4.17)  
(33) 優先権主張国 日本 (J P)

(71) 出願人 000005821  
松下電器産業株式会社  
大阪府門真市大字門真1006番地  
(72) 発明者 布田 裕一  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内  
(72) 発明者 小野 貴敏  
愛知県名古屋市中区栄2丁目6番1号 白  
川ビル別館5階 株式会社松下電器情報シ  
ステム名古屋研究所内  
(74) 代理人 100090446  
弁理士 中島 司朗

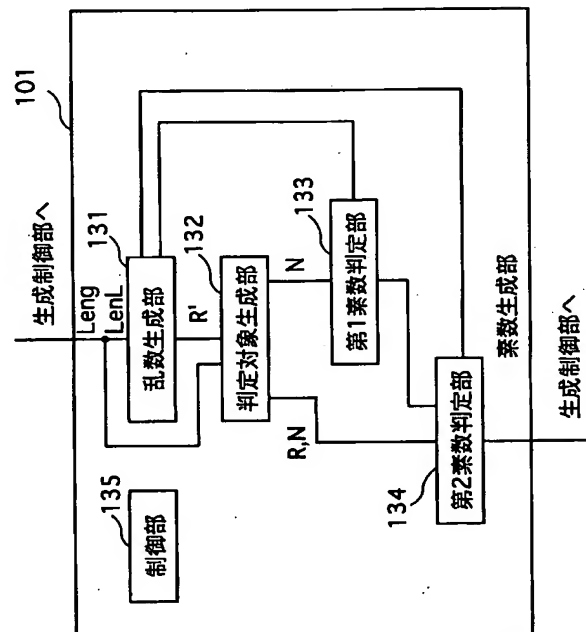
最終頁に続く

(54) 【発明の名称】 情報セキュリティ装置、素数生成装置及び素数生成方法

(57) 【要約】

【課題】 計算量が少なく、かつ、確定的に素数生成が可能な素数生成装置を提供する。

【解決手段】 情報セキュリティ装置は、素数  $q$  を入力とし、 $q$  より大きな素数  $N$  を生成する。 $2 \times u \times q + 1 \neq 0 \pmod{L_i}$  ( $i=1, 2, \dots, n$ ) を満たす数  $u$  を生成する部分情報設定部と、乱数  $R'$  を生成する乱数生成部と、数  $u$  と、乱数  $R'$  を用いて、 $R = u + L_1 \times L_2 \times \dots \times L_n \times R'$  と、 $N = 2 \times R \times q + 1$  を生成する判定対象生成部と、数  $N$  及び数  $R$  を用いて素数判定する素数判定部を備える。



## 【特許請求の範囲】

【請求項1】 素因数分解することが計算量の上で困難であることを根拠として、2個の素数を生成し生成した2個の素数の乗算を用いて、所定の情報を安全かつ確実に扱い、各素数生成の際に、既知の素数 $q$ の2倍のビット長を有する素数 $N$ を生成する情報セキュリティ装置であって、

素数 $q$ 及び $n$ 個の素数 $L_1, L_2, \dots, L_n$ を取得し、ここで、素数 $L_1, L_2, \dots, L_n$ は、それぞれ素数 $q$ より小さい2以外の素数であり、素数 $q$ は、 $q = 1 \bmod L_i$  ( $i = 1, 2, \dots, n$ ) を満たす取得手段と、

取得した前記素数 $L_1, L_2, \dots, L_n$ に係る数を除外した選択により、取得した前記素数 $q$ の2倍のビット長を有する数 $N$ を生成する生成手段と、生成した数 $N$ の素数判定を行い、数 $N$ が素数であると判定とされた場合に、数 $N$ を素数として出力する判定手段とを備えることを特徴とする情報セキュリティ装置。

【請求項2】 前記生成手段は、

$N = 1 \bmod L_i$  ( $i = 1, 2, \dots, n$ ) を満たす前記数 $N$ を生成することを特徴とする請求項1に記載の情報セキュリティ装置。

【請求項3】 前記生成手段は、

( $L_n q - L_n L - 1$ ) ビット長の乱数 $R'$ を生成し、ここで、 $L_n q$ は、素数 $q$ のビット長であり、 $L_n L$ は、( $L_1 \times L_2 \times \dots \times L_n$ ) のビット長である乱数生成部と、

生成した $R'$ 及び前記素数 $L_1, L_2, \dots, L_n$ を用いて、数 $R = L_1 \times L_2 \times \dots \times L_n \times R'$ により、数 $R$ を生成し、取得した素数 $q$ 及び生成した数 $R$ を用いて、数 $N = 2 \times R \times q + 1$ を生成する判定対象生成部とを含み、

前記判定手段は、前記数 $N$ 及び前記数 $R$ を用いて、前記数 $N$ の素数判定を行うことを特徴とする請求項2に記載の情報セキュリティ装置。

【請求項4】 前記判定手段は、生成した前記数 $N$ について、

第1判定式  $2^{N-1} = 1 \bmod N$

が成立するか否かを判定し、

さらに、生成した前記数 $N$ 及び前記数 $R$ について、

第2判定式  $2^{2R} \neq 1 \bmod N$

が判定するか否かを判定し、

第1判定式及び第2判定式の両方が成立する場合に、数 $N$ が素数であると判定することを特徴とする請求項3に記載の情報セキュリティ装置。

【請求項5】 前記生成手段は、

取得した前記素数 $q$ を用いて、

$2 \times u \times q + 1 \neq 0 \bmod L_i$  ( $i = 1, 2, \dots, n$ )

を満たす数 $u$ を生成する部分情報生成部と、

乱数 $R'$ を生成する乱数生成部と、

取得した前記素数 $L_1, L_2, \dots, L_n$ と、生成した前記数 $u$ と、生成した前記乱数 $R'$ を用いて、

$R = u + L_1 \times L_2 \times \dots \times L_n \times R'$

により、数 $R$ を生成し、取得した前記素数 $q$ と、生成した数 $R$ とを用いて、

$N = 2 \times R \times q + 1$

により、数 $N$ を生成する判定対象生成部とを含み、

前記判定手段は、前記数 $N$ 及び前記数 $R$ を用いて、前記数 $N$ の素数判定を行うことを特徴とする請求項1に記載の情報セキュリティ装置。

【請求項6】 前記部分情報生成部は、

整数 $N_1$  ( $1 \leq N_1 \leq L_1 - 1$ )、整数 $N_2$  ( $1 \leq N_2 \leq L_2 - 1$ )、 $\dots$ 、

整数 $N_n$  ( $1 \leq N_n \leq L_n - 1$ )を生成し、

数 $u_i = (N_i - 1) / (2 \times (q \bmod L_i)) \bmod L_i$  ( $i = 1, 2, \dots, n$ )

を算出する整数生成部と、

算出した前記数 $u_i$  ( $i = 1, 2, \dots, n$ )を用い

て、

数 $u = u_i \bmod L_i$  ( $i = 1, 2, \dots, n$ )

を満たす数 $u$ を算出する情報合成部とを含むことを特徴とする請求項5に記載の情報セキュリティ装置。

【請求項7】 前記判定手段は、生成した前記数 $N$ について、

第1判定式  $2^{N-1} = 1 \bmod N$

が成立するか否かを判定し、

さらに、生成した前記数 $N$ 及び前記数 $R$ について、

第2判定式  $2^{2R} \neq 1 \bmod N$

が判定するか否かを判定し、

第1判定式及び第2判定式の両方が成立する場合に、数 $N$ が素数であると判定することを特徴とする請求項6に記載の情報セキュリティ装置。

【請求項8】 素因数分解することが計算量の上で困難であることを根拠として、2個の素数を生成し生成した2個の素数の乗算を用いて、所定の情報を安全かつ確実に扱い、各素数生成の際に、既知の素数 $q$ の2倍のビット長を有する素数 $N$ を生成するICカードであって、

素数 $q$ 及び $n$ 個の素数 $L_1, L_2, \dots, L_n$ を取得し、ここで、素数 $L_1, L_2, \dots, L_n$ は、それぞれ素数 $q$ より小さい2以外の素数であり、素数 $q$ は、 $q = 1 \bmod L_i$  ( $i = 1, 2, \dots, n$ ) を満たす取得手段と、

取得した前記素数 $L_1, L_2, \dots, L_n$ に係る数を除外した選択により、取得した前記素数 $q$ の2倍のビット長を有する数 $N$ を生成する生成手段と、

生成した数 $N$ の素数判定を行い、数 $N$ が素数であると判定とされた場合に、数 $N$ を素数として出力する判定手段とを備えることを特徴とするICカード。

【請求項9】 既知の素数 $q$ の2倍のビット長を有する

素数  $N$  を生成する素数生成装置であって、  
素数  $q$  及び  $n$  個の素数  $L_1, L_2, \dots, L_n$  を取得し、ここで、素数  $L_1, L_2, \dots, L_n$  は、それぞれ素数  $q$  より小さい 2 以外の素数であり、素数  $q$  は、 $q = 1 \bmod L_i$  ( $i = 1, 2, \dots, n$ ) を満たす取得手段と、  
取得した前記素数  $L_1, L_2, \dots, L_n$  に係る数を除外した選択により、取得した前記素数  $q$  の 2 倍のビット長を有する数  $N$  を生成する生成手段と、  
生成した数  $N$  の素数判定を行い、数  $N$  が素数であると判定とされた場合に、数  $N$  を素数として出力する判定手段とを備えることを特徴とする素数生成装置。

【請求項 10】 既知の素数  $q$  の 2 倍のビット長を有する素数  $N$  を生成する素数生成装置で用いられる素数生成方法であって、

素数  $q$  及び  $n$  個の素数  $L_1, L_2, \dots, L_n$  を取得し、ここで、素数  $L_1, L_2, \dots, L_n$  は、それぞれ素数  $q$  より小さい 2 以外の素数であり、素数  $q$  は、 $q = 1 \bmod L_i$  ( $i = 1, 2, \dots, n$ ) を満たす取得ステップと、

取得した前記素数  $L_1, L_2, \dots, L_n$  に係る数を除外した選択により、取得した前記素数  $q$  の 2 倍のビット長を有する数  $N$  を生成する生成ステップと、  
生成した数  $N$  の素数判定を行い、数  $N$  が素数であると判定とされた場合に、数  $N$  を素数として出力する判定ステップとを含むことを特徴とする素数生成方法。

【請求項 11】 既知の素数  $q$  の 2 倍のビット長を有する素数  $N$  を生成するコンピュータで用いられる素数生成プログラムであって、

素数  $q$  及び  $n$  個の素数  $L_1, L_2, \dots, L_n$  を取得し、ここで、素数  $L_1, L_2, \dots, L_n$  は、それぞれ素数  $q$  より小さい 2 以外の素数であり、素数  $q$  は、 $q = 1 \bmod L_i$  ( $i = 1, 2, \dots, n$ ) を満たす取得ステップと、

取得した前記素数  $L_1, L_2, \dots, L_n$  に係る数を除外した選択により、取得した前記素数  $q$  の 2 倍のビット長を有する数  $N$  を生成する生成ステップと、  
生成した数  $N$  の素数判定を行い、数  $N$  が素数であると判定とされた場合に、数  $N$  を素数として出力する判定ステップとを含むことを特徴とする素数生成プログラム。

【請求項 12】 既知の素数  $q$  の 2 倍のビット長を有する素数  $N$  を生成するコンピュータで用いられる素数生成プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、

前記素数生成プログラムは、

素数  $q$  及び  $n$  個の素数  $L_1, L_2, \dots, L_n$  を取得し、ここで、素数  $L_1, L_2, \dots, L_n$  は、それぞれ素数  $q$  より小さい 2 以外の素数であり、素数  $q$  は、 $q = 1 \bmod L_i$  ( $i = 1, 2, \dots, n$ ) を満たす取得ステップと、

取得した前記素数  $L_1, L_2, \dots, L_n$  に係る数を除外した選択により、取得した前記素数  $q$  の 2 倍のビット長を有する数  $N$  を生成する生成ステップと、  
生成した数  $N$  の素数判定を行い、数  $N$  が素数であると判定とされた場合に、数  $N$  を素数として出力する判定ステップとを含むことを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、素数生成を用いて実現する情報セキュリティ技術に関する。

【0002】

【従来の技術】 近年、コンピュータ技術及び通信技術に基づくデータ通信が広く普及してきており、このデータ通信においては、秘密通信方式やデジタル署名方式が用いられる。ここで、秘密通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行なう方式である。またデジタル署名方式とは、通信相手に通信内容の正当性を示したり、発信者の身元を証明する通信方式である。

20 【0003】 1. 公開鍵暗号方式

これらの秘密通信方式又はデジタル署名方式においては、公開鍵暗号方式とよばれる暗号方式が用いられる。公開鍵暗号方式は通信相手が多数のとき、通信相手ごとに異なる暗号鍵を容易に管理するための方式であり、多数の通信相手と通信を行なうのに不可欠な基盤技術である。公開鍵暗号方式を用いる秘密通信では、暗号化鍵と復号化鍵とが異なり、復号化鍵は秘密にするが、暗号化鍵は公開する。秘密にする復号化鍵を秘密鍵と呼び、公開する暗号化鍵を公開鍵と呼ぶ。

30 【0004】 公開鍵暗号方式の 1 種である RSA 暗号方式では、整数の素因数分解問題を解くことが、計算量の上で困難であることを安全性の根拠としている。素因数分解問題とは、 $p, q$  を素数とし、整数  $n = p \times q$  とするとき、整数  $n$  に対して、素数  $p, q$  を求める問題である。ここで、 $\times$  は通常の乗算である。なお、素因数分解問題については、岡本龍明、太田和夫共編、「暗号・ゼロ知識問題・数論」、共立出版、1990、144～151 ページに詳しく述べられている。

40 【0005】 (素因数分解問題を応用する RSA 暗号方式) 素因数分解問題を応用する RSA 暗号方式について説明する。

(1) 鍵の生成

次に示すようにして公開鍵及び秘密鍵を計算する。

・ランダムに大きい素数  $p, q$  を選択し、その積  $n = p \times q$  を計算する。

【0006】 ・  $(p-1)$  及び  $(q-1)$  の最小公倍数  $L = \text{LCM}(p-1, q-1)$  を計算する。

・  $L$  と互いに素で  $L$  より小さい整数  $e$  をランダムに選ぶ。

50  $1 \leq e \leq L-1, \text{GCD}(e, L) = 1$

ここで、 $GCD(e, L)$  は、 $e$  及び  $L$  の最大公約数を示している。

【0007】  $d = e^{-1} \bmod L$  を計算する。このようにして、得られた整数  $e$  及び整数  $n$  が、公開鍵である。また、整数  $d$  が、秘密鍵である。

## (2) 暗号文の生成

公開鍵である整数  $e$  及び整数  $n$  を用いて、平文  $m$  に暗号演算を施して暗号文  $c$  を計算する。

【0008】  $c = m^e \bmod n$

## (3) 復号文の生成

秘密鍵である整数  $d$  を用いて、暗号文  $c$  に復号演算を施して復号文  $m'$  を計算する。

$m' = c^d \bmod n$

なお、

$m' = c^d \bmod n$

$= (m^e)^d \bmod n$

$= m^{*} (e \times d \bmod L) \bmod n$

$= m^1 \bmod n$

$= m \bmod n$

であるので、復号文  $m'$  は、平文  $m$  と一致する。

【0009】 なお、この明細書において、演算子  $*$  は、べき乗を示す。例えば、 $A * x$  は、 $A^x$  であり、 $A$  を  $x$  回乗することを示す。また、RSA暗号については、岡本龍明、山本博資、「現代暗号」、産業図書、1997、110～113ページに詳しく説明されている。

## 2. 従来例1－確率的素数生成方法

上記に示した素因数分解を応用したRSA暗号における公開鍵の生成のステップにおいて、素数生成が行われる。素数生成については、A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, "Handbook of applied cryptography", CRC Press, 1997, 145～154ページに詳しく説明されている。

【0010】 従来技術としての確率的素数生成方法について、説明する。この確率的素数生成方法は、素数判定法であるMiller-Rabin法を応用している。Miller-Rabin法については、A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, "Handbook of applied cryptography", CRC Press, 1997, 138～140ページに詳しく説明されている。この素数判定法による判定される素数は、「素数である確率が高い」数であり、100%素数であるとは限らないということに注意しておく。

【0011】 あらかじめ自然数  $x$  と、小さい素数  $L_1, L_2, \dots, L_n$  とが与えられているものとする。ここで、小さい素数の一例は、「2, 3, 5, 7」である。前記確率的素数生成方法では、次に示すステップを繰り返すことにより、素数を生成する。

(ステップ1) 初期値として、自然数  $x$  を変数  $N$  に代入する。

【0012】 (ステップ2) 変数  $N$  より大きい数のう

ち、素数  $L_1, L_2, \dots, L_n$  のいずれでも割り切れない数であって、最も小さい数を得、得られた数を変数  $N$  に代入する。

(ステップ3) Miller-Rabin法により変数  $N$  の値が素数であるか否かを判定する。ここで、変数  $N$  に対して素数判定を10回繰り返す。判定の結果、素数であると判定される場合には、変数  $N$  の値を素数として出力する。素数でないと判定される場合には、ステップ2へ戻って、素数が出力されるまで、処理を繰り返す。

10 【0013】 上記のように、小さい素数2, 3, 5, 7で割り切れない数を求める理由は、ステップ3の素数判定の回数を減らすためである。即ち、素数判定する対象となる数を2, 3, 5, 7で割り切れない数だけに絞っている。 $2 \times x + 1 \bmod 210$  が2, 3, 5, 7で割り切れない数は47個あるため、上記のように、2, 3, 5, 7で割り切れない数のみを対象として素数判定すると、素数判定する回数は、 $47/210$  に削減できる。

20 【0014】 しかしながら、ステップ2により得られた変数  $N$  の値が合成数(素数でない数)であるとき、Miller-Rabin法による素数判定が成立する確率は、 $1/4$  以下であることが知られている。このように、得られた変数  $N$  の値が合成数であっても、Miller-Rabin法による素数判定が成立する可能性がある。そのため、前記確率的素数生成方法は、確率的にのみ素数を生成でき、確定的に素数を生成できないという問題がある。

30 【0015】 (確率的素数生成方法の計算量) 次に、前記確率的素数生成方法を用いて素数を生成する場合の計算量について説明する。ここでは、冪乗剰余演算の回数で計算量を見積もるものとする。前記確率的素数生成方法では、上述したように、素数と思われる数に対しては、Miller-Rabin法による素数判定を10回繰り返す。以下では、合成数に対して行われるMiller-Rabin法による素数判定の回数の平均を求める。

【0016】 第  $i$  回目の素数判定試行を行う確率を  $P_i$  とすると、第  $i+1$  回目の素数判定試行を行う確率  $P_{i+1}$  は、第  $i$  回の  $P_i$  の確率で素数判定試行を行い、かつ  $1/4$  以下の確率でさらに素数判定試行を行う確率である。従って、

$$P_{i+1} \leq P_i \times 1/4$$

である。第1回目の素数判定試行は、必ず行うため、その確率は1であるので、 $P_1 = 1$  である。よって、

$$P_i \leq (1/4)^{*(i-1)}$$

である。

【0017】 Miller-Rabin法による素数判定1回につき、冪乗剰余演算を1回行う。前記確率的素数生成方法では、Miller-Rabin法による素数判定を最大で10回行うため、1つの合成数に対する冪乗剰余演算回数の平均値は、

50 【0018】

7

【数1】  

$$\sum_{i=1}^{10} P_i \leq \sum_{i=1}^{10} (1/4) ** (i-1) = 1.33$$

【0019】である。一般にNを任意に選ぶとき、Nが素数となる確率は、 $1/(1 \ln N)$ 程度であるので、平均的には、 $1 \ln N$ 回の素数判定を行うと素数を発見できることになる。ここで、 $1 \ln N$ は、Nの自然対数である。しかし、2、3、5、7で割り切れる数は予め除外しているので、その回数は、 $\phi(2 \times 3 \times 5 \times 7) / 210 = 48/210$ に削減できる。ここで、 $\phi(2 \times 3 \times 5 \times 7)$ は、210未満の自然数の2、3、5、\*

$$(8/35 \times (1 \ln N) - 1) \times (\sum_{i=1}^{10} 1/(4 ** (n-1))) + 10$$

【0022】以下である。例えば、Nが512ビットのとき、多くとも116.8回であることが保証されている。素数判定を行う数を2、3、5、7で割り切れない数に絞込まない場合、即ち、全ての数を素数判定を行※

$$(1 \ln N - 1) \times (\sum_{i=1}^{10} 1/(4 ** (n-1))) + 10$$

【0024】以下である。Nが512ビットのとき、この値は481.9になる。以上より、従来例1は、冪乗剰余演算回数が約1/4に削減できる。しかしながら、上述したように、確定的に素数を出力できない。

### 3. 従来例2-確定的素数生成方法

確定的に素数を生成することができるMaurer法による確定的素数生成方法について説明する。ここで、Maurer法については、A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, "Handbook of applied cryptography", CRC Press, 1997, 152~153ページに詳しく説明されている。

【0025】前記確定的素数生成方法では、次に示すステップを繰り返すことにより、素数を生成する。あらかじめサイズLenqの素数qが与えられている。

(ステップ1) Lenq-1ビットの乱数Rを選択する。なお、乱数Rの先頭ビットは、必ず1となるようにする。

【0026】(ステップ2) 数Nを以下の式により計算する。

$$N = 2 \times q \times R + 1$$

(ステップ3) 数Nが素数であるか否かを、次に示す第1判定及び第2判定がともに、成立する場合に、素数と判定する。他の場合に、素数でないと判定する。

8

\*7と互いに素な数の個数を示している。従って、素数判定を行う数(合成数と最後の素数と思われる数)の個数は、

$$8/35 \times (1 \ln N)$$

である。その中で、最後の数が素数であると考え、素数判定を行う合成数の個数は、

$$(8/35 \times (1 \ln N)) - 1$$

となる。

【0020】以上より、冪乗剰余演算の回数は、平均的に、

【0021】

【数2】

20 ※う対象にする場合、冪乗剰余演算の回数は、平均的に、

【0023】

【数3】

【0027】

(第1判定)  $2^{N-1} = 1 \pmod N$

(第2判定)  $\text{GCD}(2^{2^R} - 1, N) = 1$

素数であると判定される場合には、数Nを素数として出力する。素数でないと判定される場合には、ステップ1へ戻って、素数が出力されるまで、処理を繰り返す。

【0028】この判定方法は、Pocklingtonの素数判定法とよばれ、A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, "Handbook of applied cryptography", CRC Press, 1997, 144ページに詳しく述べられている。Pocklingtonの素数判定法では、 $N = 2 \times q \times R + 1$ のqが素数であり、第1判定及び第2判定の結果が真であれば、必ず、Nが素数になる。そのため、確定的に素数であることを判定でき、確定的な素数生成が可能になる。

【0029】このようにして、Maurer法による確定的素数生成方法では、サイズLenqの素数qを基にして、サイズ $2 \times \text{Lenq}$ の素数Nを生成する。従って、Maurer法による確定的素数生成方法を用いて所定長の素数を生成する場合には、前記所定長以下の素数の生成を繰り返し行う。例えば、512ビット長の素数を生成する場合には、あらかじめ与えられた8ビットの素数を基にして16ビットの素数を生成する。次に、生成した16ビットの素数を基にして32ビットの素数

を生成する。次に、生成した 32 ビットの素数を基にして 64 ビットの素数を生成する。以下同様の素数生成を繰り返して、512 ビットの素数を生成する。

【0030】なお、前記第 2 判定を次の判定に代えてもよい。

$$2^{2R} \neq 1 \pmod{N}$$

(確定的素数生成方法の計算量) 次に、Maurer 法による確定的素数生成方法を用いて素数を生成する場合の計算量について説明する。

【0031】ここでは、512 ビットの数の冪乗剰余演算の回数で計算量を見積もる。つまり、256 ビットの素数を用いて、512 ビットの素数を生成する場合について考える。一般に、正整数 R を任意に選ぶとき、正整数 R が素数となる確率は、 $1 / (\ln R)$  程度であるので、この場合、512 ビットの素数を生成するために Pocklington 判定を試す回数は、 $\ln 2^{512}$  と見積もることができる。従来例 2 では奇数のみに対して、素数判定を行うので、この個数は、 $(\ln 2^{512}) / 2$  となる。

【0032】次に、前記第 1 判定を通過する確率は、Miller-Rabin 判定を通過する確率と等しく、 $1 / 4$  以下である。従って、1 つの合成数に対して行う冪乗剰余演算の回数は、 $1 + 1 / 4$  以下である。当然、素数に対して行う冪乗剰余演算回数は、2 である。以上より、256 ビットの素数を用いて、512 ビットの素数を生成するために行う 512 ビットの冪乗剰余演算回数は、

$$(1 + 1/4) \cdot ((\ln 2^{512}) / 2 - 1) + 2 = 22.6$$

以下である。

【0033】128 ビットから 256 ビットの素数を生成する場合も同様に考えると、256 ビットの冪乗剰余演算における判定回数は、 $(\ln 2^{256}) / 2$  であり、256 ビットの素数を生成するために行う 256 ビットの冪乗剰余演算回数は、

$$(1 + 1/4) \cdot ((\ln 2^{256}) / 2 - 1) + 2$$

以下である。冪乗剰余演算の計算量は、法 N に依存し、N の 3 乗のオーダーである。従って、256 ビットの冪乗剰余演算 8 回を、512 ビットの冪乗剰余演算 1 回相当と考える。

【0034】64 ビットから 128 ビットなどの他も同様に考えると、従来例 2 全体の計算量を、512 ビットの冪乗剰余演算回数で見積もることができる。16、32 ビットの素数生成の計算量は、64、128、256、512 ビットの素数生成の計算量に比べて小さいため無視し、従来例 2 全体の計算量を、512 ビットの冪乗剰余演算回数で表すと、

$$(1 + 1/4) \times \{ (\ln 2^{64}) / 2 - 1 / 512 + ((\ln 2^{128}) / 2 - 1) / 64 + ((\ln 2^{256}) / 2 - 1) / 8 + ((\ln 2^{512}) / 2 - 1) \} + 2 (1 / 512 + 1 / 64 + 1 / 8 +$$

$$1) = 237.4$$

以下である。

【0035】従来例 2 における計算量は、従来例 1 の 116.8 回以下に比べれば、計算量が 2 倍以上多いことになる。以上説明したように、従来例 2 によると、確定的な素数生成が可能であるが、従来例 1 より計算量が多い。

【0036】

【発明が解決しようとする課題】このように、計算量が少ない素数生成法では、確定的に素数生成ができないという問題がある。また、確定的に素数生成が可能な素数法では、計算量が多いという問題がある。本発明は、上記の問題点を解決し、計算量が少なく、かつ、確定的に素数生成が可能な素数生成装置、素数生成方法、素数生成プログラム、素数生成プログラムを記録している記録媒体及び情報セキュリティ装置を提供することを目的とする。

【0037】

【課題を解決するための手段】上記目的を達成するために、本発明は、素因数分解をすることが計算量の上で困難であることを根拠として、2 個の素数を生成し生成した 2 個の素数の乗算を用いて、所定の情報を安全かつ確実に扱い、各素数生成の際に、既知の素数 q の 2 倍のビット長を有する素数 N を生成する情報セキュリティ装置であって、素数 q 及び n 個の素数  $L_1$ 、 $L_2$ 、 $\dots$ 、 $L_n$  を取得し、ここで、素数  $L_1$ 、 $L_2$ 、 $\dots$ 、 $L_n$  は、それぞれ素数 q より小さい 2 以外の素数であり、素数 q は、 $q = 1 \pmod{L_i}$  ( $i = 1, 2, \dots, n$ ) を満たす取得手段と、取得した前記素数  $L_1$ 、 $L_2$ 、 $\dots$ 、 $L_n$  に係る数を除外した選択により、取得した前記素数 q の 2 倍のビット長を有する数 N を生成する生成手段と、生成した数 N の素数判定を行い、数 N が素数であると判定とされた場合に、数 N を素数として出力する判定手段とを備える。

【0038】ここで、前記生成手段は、 $N = 1 \pmod{L_i}$  ( $i = 1, 2, \dots, n$ ) を満たす前記数 N を生成するように構成してもよい。ここで、前記生成手段は、 $(\text{Len } q - \text{Len } L - 1)$  ビット長の乱数  $R'$  を生成し、ここで、 $\text{Len } q$  は、素数 q のビット長であり、 $\text{Len } L$  は、 $(L_1 \times L_2 \times \dots \times L_n)$  のビット長である乱数生成部と、生成した  $R'$  及び前記素数  $L_1$ 、 $L_2$ 、 $\dots$ 、 $L_n$  を用いて、数  $R = L_1 \times L_2 \times \dots \times L_n \times R'$  により、数 R を生成し、取得した素数 q 及び生成した数 R を用いて、数  $N = 2 \times R \times q + 1$  を生成する判定対象生成部とを含み、前記判定手段は、前記数 N 及び前記数 R を用いて、前記数 N の素数判定を行うように構成してもよい。

【0039】ここで、前記判定手段は、生成した前記数 N について、第 1 判定式  $2^{N-1} = 1 \pmod{N}$  が成立するか否かを判定し、さらに、生成した前記数 N 及



び前記数Rについて、第2判定式  $2^{2R} \neq 1 \pmod{N}$  が判定するか否かを判定し、第1判定式及び第2判定式の両方が成立する場合に、数Nが素数であると判定するように構成してもよい。

【0040】ここで、前記生成手段は、取得した前記素数qを用いて、 $2 \times u \times q + 1 \neq 0 \pmod{L_i}$  ( $i = 1, 2, \dots, n$ ) を満たす数uを生成する部分情報生成部と、乱数R'を生成する乱数生成部と、取得した前記素数 $L_1, L_2, \dots, L_n$ と、生成した前記数uと、生成した前記乱数R'を用いて、 $R = u + L_1 \times L_2 \times \dots \times L_n \times R'$ により、数Rを生成し、取得した前記素数qと、生成した数Rとを用いて、 $N = 2 \times R \times q + 1$ により、数Nを生成する判定対象生成部とを含み、前記判定手段は、前記数N及び前記数Rを用いて、前記数Nの素数判定を行うように構成してもよい。

【0041】ここで、前記部分情報生成部は、整数 $N_1$  ( $1 \leq N_1 \leq L_1 - 1$ )、整数 $N_2$  ( $1 \leq N_2 \leq L_2 - 1$ )、 $\dots$ 、整数 $N_n$  ( $1 \leq N_n \leq L_n - 1$ )を生成し、数 $u_i = (N_i - 1) / (2 \times (q \pmod{L_i})) \pmod{L_i}$  ( $i = 1, 2, \dots, n$ )を算出する整数生成部と、算出した前記数 $u_i$  ( $i = 1, 2, \dots, n$ )を用いて、数 $u = u_i \pmod{L_i}$  ( $i = 1, 2, \dots, n$ )を満たす数uを算出する情報合成部とを含むように構成してもよい。

#### 【0042】

##### 【発明の実施の形態】 1. 第1の実施の形態

本発明に係る1の実施の形態としてのコンテンツ配信システム1について、説明する。

##### 1. 1 コンテンツ配信システム1の構成

コンテンツ配信システム1は、図1に示すように、メモリカード10、携帯情報端末装置(以下、PDAと呼ぶ。)20、ヘッドフォン21、パーソナルコンピュータ(以下、PCと呼ぶ。)30、配信サーバ装置40及び携帯電話50から構成されている。

【0043】配信サーバ装置40は、音楽であるデジタル著作物を暗号化して暗号化デジタル著作物を得、得られた暗号化デジタル著作物を、インターネット60を介して、PC30へ送信し、PC30は、暗号化デジタル著作物を受信する。利用者は、メモリカード10をPC30に装着し、PC30は、受信した暗号化デジタル著作物をメモリカード10へ書き込む。メモリカード10は、暗号化デジタル著作物を復号して、デジタル著作物を生成し、生成したデジタル著作物を記憶する。次に、利用者は、暗号化デジタル著作物が書き込まれているメモリカード10をPDA20に装着する。PDA20には、ヘッドフォン21が接続されており、PDA20は、メモリカード10に書き込まれているデジタル著作物を変換して電気信号を生成し、生成した電気信号をヘッドフォン21へ出力する。ヘッドフォン21は、電気

信号を音声に変換して、音声を出力する。

【0044】また、配信サーバ装置40は、音楽であるデジタル著作物を暗号化して暗号化デジタル著作物を得、得られた暗号化デジタル著作物を、インターネット60、携帯電話網62及び無線基地局61を介して、携帯電話50へ送信し、携帯電話50は、暗号化デジタル著作物を受信する。利用者は、メモリカード10を携帯電話50に装着し、携帯電話50は、受信した暗号化デジタル著作物をメモリカード10へ書き込む。メモリカード10は、書き込まれている暗号化デジタル著作物を復号して、音楽であるデジタル著作物を生成して、生成したデジタル著作物を記憶する。携帯電話50は、メモリカード10に記憶されているデジタル著作物を変換して電気信号を生成し、生成した電気信号を音声に変換して、音声を出力する。

【0045】このようにして、利用者は、配信サーバ装置40から音楽であるデジタル著作物を受信して、楽しむことができる。

##### 1. 2 メモリカード10

メモリカード10は、図2に示すように、素数生成部101、生成制御部102、素数記憶部103、乱数生成部104、秘密鍵記憶部105、公開鍵生成部106、公開鍵記憶部107、復号部108、メモリ部109、制御部112、認証部113及び送受信部114から構成されている。

【0046】メモリカード10は、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記RAMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、メモリカード10は、その機能を達成する。

##### 【0047】(1) 秘密鍵記憶部105

秘密鍵記憶部105は、秘密鍵としての数nと数dとを記憶するための領域を備えている。

##### (2) 公開鍵記憶部107

公開鍵記憶部107は、公開鍵としての数nと数eとを記憶するための領域を備えている。

##### 【0048】(3) メモリ部109

メモリ部109は、一般領域111とセキュア領域110とから構成されている。一般領域111及びセキュア領域110は、それぞれ情報を記憶するための領域である。一般領域111は、外部からの情報の自由な書き込みと、情報の自由な読み出しが許可される領域である。一方、セキュア領域110は、認証部113により、メモリカード10が装着される相手の装置の正当性が認証された場合にのみ、情報の書き込み及び情報の読み出しが許可される領域である。

##### 【0049】(4) 素数記憶部103

素数記憶部103は、素数 $p_a$ 及び素数 $p_b$ を記憶するための領域を備えている。

## (5) 生成制御部102

生成制御部102は、素数生成部101へ、素数 $q$ と、素数 $q$ のビットサイズ $Len_q$ と、2以外の小さな素数である $L_1$ 、 $L_2$ 、 $\dots$ 、 $L_n$ と、 $(L_1 \times L_2 \times \dots \times L_n)$ のビットサイズ $Len_L$ とを出力し、次に、素数生成部101から1個の素数 $p$ を受け取り、受け取った素数 $p$ を素数 $p_a$ として素数記憶部103へ書き込む。

【0050】次に、同様にして、素数生成部101へ、素数 $q$ と、素数 $q$ のビットサイズ $Len_q$ と、2以外の小さな素数である $L_1$ 、 $L_2$ 、 $\dots$ 、 $L_n$ と、 $(L_1 \times L_2 \times \dots \times L_n)$ のビットサイズ $Len_L$ とを出力し、次に、素数生成部101から1個の素数 $p$ を受け取り、受け取った素数 $p$ を素数 $p_b$ として素数記憶部103へ書き込む。

【0051】なお、素数 $q$ と、素数 $q$ のビットサイズ $Len_q$ と、2以外の小さな素数である $L_1$ 、 $L_2$ 、 $\dots$ 、 $L_n$ と、 $(L_1 \times L_2 \times \dots \times L_n)$ のビットサイズ $Len_L$ については、後述する。上記に説明しているように、生成制御部102は、素数生成部101を2回、制御することにより、2個の素数を生成している。後述するように、素数生成部101により素数を生成するプロセスにおいて、乱数を用いているので、生成された2個の素数が偶然一致する可能性は、低いと考えられる。しかしながら、生成された2個の素数が偶然一致した場合において、生成制御部102は、再度2回目の素数生成をするように、素数生成部101を制御し、必ず異なる2個の素数を採用するようにしてもよい。

【0052】また、生成制御部102は、前記2回の素数生成の際に、素数 $q$ と、ビットサイズ $Len_q$ と、素数 $L_1$ 、 $L_2$ 、 $\dots$ 、 $L_n$ と、ビットサイズ $Len_L$ とからなるパラメタ群を用いるとしているが、2回の素数生成の際に異なるパラメタ群を用いてもよい。つまり、1回めの素数生成の際に、素数 $q$ と、ビットサイズ $Len_q$ と、 $n$ 個の素数 $L_1$ 、 $L_2$ 、 $\dots$ 、 $L_n$ と、ビットサイズ $Len_L$ とからなるパラメタ群を用いる。次に、2回めの素数生成の際に、素数 $q'$ と、素数 $q'$ のビットサイズ $Len_{q'}$ と、 $j$ 個の2以外の小さな素数である $L_1'$ 、 $L_2'$ 、 $\dots$ 、 $L_j'$ と、 $(L_1' \times L_2' \times \dots \times L_j')$ のビットサイズ $Len_{L'}$ とからなるパラメタ群を用いてもよい。

【0053】ここで、素数 $q \neq$ 素数 $q'$ であり、 $n \neq j$ である。また、素数 $(L_1, L_2, \dots, L_n) \neq$ 素数 $(L_1', L_2', \dots, L_j')$ である。これは、素数 $(L_1, L_2, \dots, L_n)$ と、素数 $(L_1', L_2', \dots, L_j')$ の少なくとも1個が異なっていることを示している。

## (6) 素数生成部101

素数生成部101は、図3に示すように、乱数生成部131、判定対象生成部132、第1素数判定部133、第2素数判定部134及び制御部135から構成されて

いる。

【0054】素数生成部101は、

$$q = 1 \bmod L_1,$$

$$q = 1 \bmod L_2,$$

$$\dots q = 1 \bmod L_n \text{ を満たす素数 } q \text{ と、}$$

素数 $q$ のビットサイズ $Len_q$ とが与えられたとき、素数 $q$ のビットサイズの2倍のビットサイズをもつ素数 $p$ を出力する。

【0055】ここで、 $L_1$ 、 $L_2$ 、 $\dots$ 、 $L_n$ は2以外の小さな素数である。また、 $(L_1 \times L_2 \times \dots \times L_n)$ のビットサイズ $Len_L$ は予め与えられているものであるとする。小さな素数の例として、想定する入力 $q$ のビットサイズより小さな素数、例えば $L_1 = 3$ 、 $L_2 = 5$ などが挙げられる。

【0056】(乱数生成部131) 乱数生成部131は、生成制御部102からビットサイズ $Len_q$ 及び $Len_L$ を受け取り、受け取ったビットサイズ $Len_q$ 及び $Len_L$ を用いて、 $(Len_q - Len_L - 1)$ ビットサイズの乱数 $R'$ を生成し、生成した乱数 $R'$ を判定対象生成部132へ出力する。

【0057】また、乱数生成部131は、第1素数判定部133から後述する第1判定情報を受け取る。また、第2素数判定部134から後述する第2判定情報を受け取る。乱数生成部131は、第1判定情報、又は第2判定情報を受け取ると、再度、受け取ったビットサイズ $Len_q$ 及び $Len_L$ を用いて、 $(Len_q - Len_L - 1)$ ビットサイズの乱数 $R'$ を生成し、生成した乱数 $R'$ を判定対象生成部132へ出力する。

【0058】(判定対象生成部132) 判定対象生成部132は、生成制御部102から素数 $q$ を受け取り、乱数生成部131から乱数 $R'$ を受け取る。次に、判定対象生成部132は、受け取った素数 $q$ と乱数 $R'$ とを用いて、以下の式を満たす数 $R$ と数 $N$ とを生成する。

【0059】

$$R = L_1 \times L_2 \times \dots \times L_n \times R'$$

$$N = 2 \times R \times q + 1$$

次に、判定対象生成部132は、生成した数 $R$ を第2素数判定部134へ出力し、生成した数 $N$ を第1素数判定部133及び第2素数判定部134へ出力する。

【0060】(第1素数判定部133) 第1素数判定部133は、判定対象生成部132から数 $N$ を受け取り、受け取った数 $N$ を用いて、次に示す判定式1の成立を判定する。

$$2^{N-1} = 1 \bmod N \quad (\text{判定式1})$$

判定式1が成立する場合には、その旨を示す第1判定情報を第2素数判定部134へ出力する。判定式1が成立しない場合には、その旨を示す第1判定情報を乱数生成部131へ出力する。

【0061】(第2素数判定部134) 第2素数判定部134は、判定対象生成部132から数 $N$ と数 $R$ とを受

け取り、また、第1素数判定部133から、判定式1が成立する旨を示す第1判定情報を受け取る。判定式1が成立する旨を示す第1判定情報を受け取ると、次に、第2素数判定部134は、受け取った数Nと数Rとを用いて、次に示す判定式2の成立を判定する。

【0062】

$$2^{2R} \neq 1 \pmod{N} \quad (\text{判定式2})$$

判定式2が成立する場合には、素数pとして数Nを生成制御部102へ出力する。判定式2が成立しない場合には、その旨を示す第2判定情報を乱数生成部131へ出力する。

(制御部135) 制御部135は、素数生成部101を構成する各要素を制御する。

【0063】(素数生成部101の動作の検証) 第1素数判定部133及び第2素数判定部134による判定は、Pocklington判定である。Pocklington判定については、岡本 栄司、「暗号理論入門」、共立出版、1993、21ページ及び、A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, "Handbook of applied cryptography", CRC Press, 1997, 144ページに詳しく述べられている。

【0064】 $N = 2 \times R \times q + 1$ のqが素数であり

$$2^{N-1} = 1 \pmod{N}$$

$$2^{2R} \neq 1 \pmod{N}$$

の両方が成り立つ場合、Nが素数になるので、素数生成部101は素数Nを出力する。また、乱数R'のビットサイズが $\text{Len } q - \text{Len } L - 1$ であるので、数Rのビットサイズが $\text{Len } q - 1$ になり、数Nのビットサイズが $2 \times \text{Len } q$ になる。

【0065】(7) 公開鍵生成部106

公開鍵生成部106は、素数記憶部103から素数 $p_a$ 及び素数 $p_b$ を読み出し、読み出した素数 $p_a$ と素数 $p_b$ とを乗じて整数 $n = p_a \times p_b$ を算出し、算出した整数nを秘密鍵記憶部105及び公開鍵記憶部107へ書き込み、数 $(p_a - 1)$ と数 $(p_b - 1)$ との最小公倍数 $L = \text{LCM}(p_a - 1, p_b - 1)$ を算出する。

【0066】また、公開鍵生成部106は、乱数生成部104から乱数eを受け取り、受け取った乱数eを用いて、数 $d = e^{-1} \pmod{L}$ を算出し、算出した数dを秘密鍵記憶部105へ書き込み、乱数eを公開鍵記憶部107へ書き込む。

(8) 乱数生成部104

乱数生成部104は、乱数eを生成し、生成した乱数eを公開鍵生成部106へ出力する。

【0067】(9) 送受信部114

送受信部114は、公開鍵記憶部107から整数n及び乱数eを読み出し、読み出した整数n及び乱数eをPC30へ出力する。また、送受信部114は、配信サーバ装置40からインターネット60及びPC30を介して、暗号文cを受信し、受信した暗号文cをメモリ部109内の一般領域111へ書き込む。

【0068】(10) 復号部108

復号部108は、一般領域111から暗号文cを読み出し、秘密鍵記憶部105から数d及び整数nを読み出し、読み出した数d及び整数nを用いて、次の式により、暗号文cを復号して、復号文m'を生成する。 $m' = c^d \pmod{n}$ 次に、復号部108は、生成した復号文m'をメモリ部109内のセキュア領域110へ書き込む。

【0069】(11) 認証部113

10 認証部113は、メモリカード10が装着される相手の装置との間で、相手の装置の正当性を認証する。正当性が認証された場合に、メモリ部109内のセキュア領域110への情報の書き込み及びセキュア領域110からの情報の読み出しを許可する。

【0070】(12) 制御部112

制御部112は、メモリカード10を構成する各要素を制御する。1. 3 PC30 PC30は、図4に示すように、送受信部301、認証部302、制御部303、送受信部304、入力部305、表示部306から構成されている。

【0071】この装置は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、液晶ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、前記装置は、その機能を達成する。

【0072】PC30は、メモリカード10から整数n及び乱数eを受け取り、受け取った整数n及び乱数eを、インターネット60を介して、配信サーバ装置40へ送信する。また、PC30は、配信サーバ装置40から、インターネット60を介して、暗号文cを受け取り、受け取った暗号文cを、メモリカード10の送受信部114へ送信する。

【0073】1. 4 配信サーバ装置40

配信サーバ装置40は、図5に示すように、送受信部401、公開鍵記憶部402、暗号化部403、制御部404及び情報記憶部405から構成されている。この装置は、PC30と同様に、コンピュータシステムであり、マイクロプロセッサが、コンピュータプログラムに従って動作することにより、前記装置は、その機能を達成する。

【0074】(1) 情報記憶部405

情報記憶部405は、あらかじめ平文mを記憶している。平文mは、具体的には、デジタルの音楽情報である。

(2) 公開鍵記憶部402

50 公開鍵記憶部402は、公開鍵としての整数n及び乱数eを記憶するための領域を備えている。

## 【0075】(3) 送受信部401

送受信部401は、PC30からインターネット60を介して、整数 $n$ 及び乱数 $e$ を受信し、受信した整数 $n$ 及び乱数 $e$ を公開鍵記憶部402へ書き込む。また、送受信部401は、暗号化部403から、暗号文 $c$ を受け取り、受け取った暗号文 $c$ を、インターネット60を介して、PC30へ送信する。

## 【0076】(4) 暗号化部403

暗号化部403は、情報記憶部405から平文 $m$ を読み出し、公開鍵記憶部402から整数 $n$ 及び乱数 $e$ を読み出し、読み出した整数 $n$ 及び乱数 $e$ を用いて、次の式により、平文 $m$ を暗号化して、暗号文 $c$ を生成する。 $c = m^e \bmod n$ 次に、暗号化部403は、生成した暗号文 $c$ を送受信部401へ出力する。

## 【0077】(5) 制御部404

制御部404は、配信サーバ装置40を構成する各要素を制御する。

## 1. 5 PDA20及びヘッドフォン21

PDA20は、メモリカード10のメモリ部109内のセキュア領域110に書き込まれている復号文 $m'$ を読み出し、読み出した復号文 $m'$ をアナログの音声信号に変換し、音声信号をヘッドフォン21へ出力する。

【0078】ヘッドフォン21は、音声信号を音声に変換して出力する。

## 1. 6 携帯電話50

携帯電話50は、無線電波を用いて、他の電話機との間で通信を行うことができる携帯型の電話機としての構成を有し、さらに、PC30及びPDA20と同様の構成を有する。

【0079】この携帯電話50は、具体的には、マイクロプロセッサ、ROM、RAM、液晶ディスプレイユニット、入力部、通信部、マイク、スピーカなどから構成されるコンピュータシステムである。前記RAMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、携帯電話50は、その機能を達成する。

【0080】携帯電話50は、PC30と同様に、メモリカード10から整数 $n$ 及び乱数 $e$ を受け取り、受け取った整数 $n$ 及び乱数 $e$ を、インターネット60を介して、配信サーバ装置40へ送信する。また、携帯電話50は、配信サーバ装置40から、インターネット60を介して、暗号文 $c$ を受け取り、受け取った暗号文 $c$ を、メモリカード10の送受信部114へ送信する。

【0081】携帯電話50は、PDA20と同様に、メモリカード10に記憶されているデジタル著作物を変換して電気信号を生成し、生成した電気信号を音声に変換して、音声を出力する。

## 1. 7 コンテンツ配信システム1の動作

## (1) コンテンツ配信システム1の動作コンテンツ配信

システム1の動作について、図6に示すフローチャートを用いて説明する。

【0082】メモリカード10の素数生成部101は、ランダムに素数 $p_a$ 及び素数 $p_b$ を生成し、生成した素数 $p_a$ 及び素数 $p_b$ を素数記憶部103へ書き込む(ステップS101)。次に、公開鍵生成部106は、素数記憶部103から素数 $p_a$ 及び素数 $p_b$ を読み出し、読み出した素数 $p_a$ と素数 $p_b$ とを乗じて整数 $n = p_a \times p_b$ を算出し、算出した整数 $n$ を秘密鍵記憶部105及び公開鍵記憶部107へ書き込み、数 $(p_a - 1)$ と数 $(p_b - 1)$ との最小公倍数 $L = \text{LCM}(p_a - 1, p_b - 1)$ を算出する(ステップS102)。次に、乱数生成部104は、乱数 $e$ を生成し、生成した乱数 $e$ を公開鍵生成部106へ出力する(ステップS103)。次に、公開鍵生成部106は、乱数 $e$ を受け取り、受け取った乱数 $e$ を用いて、数 $d = e^{-1} \bmod L$ を算出し、算出した数 $d$ を秘密鍵記憶部105へ書き込み、乱数 $e$ を公開鍵記憶部107へ書き込む(ステップS104)。次に、送受信部114は、公開鍵記憶部107から整数 $n$ 及び乱数 $e$ を読み出し、読み出した整数 $n$ 及び乱数 $e$ をPC30へ出力し(ステップS105)、PC30は、整数 $n$ 及び乱数 $e$ を、インターネット60を介して、配信サーバ装置40へ送信する(ステップS106)。

【0083】配信サーバ装置40の公開鍵記憶部402は、PC30からインターネット60及び送受信部401を介して、整数 $n$ 及び乱数 $e$ を、受信して記憶し(ステップS106)、暗号化部403は、情報記憶部405から平文 $m$ を読み出し、公開鍵記憶部402から整数 $n$ 及び乱数 $e$ を読み出し、読み出した整数 $n$ 及び乱数 $e$ を用いて、次の式により、平文 $m$ を暗号化して、暗号文 $c$ を生成する。

【0084】 $c = m^e \bmod n$  (ステップS107)次に、暗号化部403は、送受信部401及びインターネット60を介して、暗号文 $c$ をPC30へ送信し(ステップS108)、PC30は、暗号文 $c$ を受け取り、受け取った暗号文 $c$ を、メモリカード10の送受信部114へ送信し、送受信部114は、受信した暗号文 $c$ をメモリ部109内の一般領域111へ書き込む(ステップS109)。復号部108は、一般領域111から暗号文 $c$ を読み出し、秘密鍵記憶部105から数 $d$ 及び整数 $n$ を読み出し、読み出した数 $d$ 及び整数 $n$ を用いて、次の式により、暗号文 $c$ を復号して、復号文 $m'$ を生成する。 $m' = c^d \bmod n$ 次に、復号部108は、生成した復号文 $m'$ をメモリ部109内のセキュア領域110へ書き込む(ステップS110)。

【0085】PDA20は、メモリカード10のメモリ部109内のセキュア領域110に書き込まれている復号文 $m'$ を読み出し(ステップS111)、読み出した

復号文 $m'$ をアナログの音声信号に変換し、音声信号をヘッドフォン21へ出力する。ヘッドフォン21は、音声信号を音声に変換して出力する(ステップS112)。

【0086】なお、メモリカード10における上記動作は、制御部112が、メモリカード10を構成する各要素を制御することにより行われる。

#### (2) 素数生成部101の動作

素数生成部101の動作について、図7に示すフローチャートを用いて説明する。

【0087】乱数生成部131は、 $Lenq - LenL - 1$ ビットの乱数 $R'$ を生成し、判定対象生成部132へ出力する(ステップS132)。次に、判定対象生成部132は、数 $R$ と数 $N$ とを計算し、数 $N$ を第1素数判定部133へ出力し、数 $N$ と数 $R$ とを第2素数判定部134に出力する(ステップS133)。次に、第1素数判定部133は、 $2^{N-1} = 1 \pmod{N}$ (判定式1)の成立を判定し、成立しない場合は(ステップS134)、ステップS132へ戻って処理を繰り返す。

【0088】成立する場合には(ステップS134)、第2素数判定部134は、 $2^{2R} \neq 1 \pmod{N}$ (判定式2)の成立を判定し、成立しない場合は(ステップS135)、ステップS132へ戻って処理を繰り返す。成立する場合は(ステップS135)、素数として数 $N$ を生成制御部102へ出力し、素数生成部101は、処理を終了する。

【0089】なお、素数生成部101における上記動作は、制御部135が、素数生成部101を構成する各要素を制御することにより行われる。

#### 1. 8 計算量の評価

素数生成部101による計算量について説明する。以下において、 $L_1 = 3$ 、 $L_2 = 5$ 、 $L_3 = 7$ 、 $n = 3$ 、 $L *$

$$\begin{aligned} & (2-1) \times (3-1) \times (5-1) \times (7-1) / (2 \times 3 \times 5 \times 7) \\ & = 48 / 210 \\ & = 8 / 35 \end{aligned}$$

となる。これは、従来例1と同じ確率である。

【0093】次に、第1素数判定部133の判定を通過する確率は、Miller-Rabin判定を通過する確率と等しく、 $1/4$ 以下である。従って、1つの合成数に対して行う冪乗剰余演算の回数は、 $1 + 1/4$ 以下である。当然、素数に対して行う冪乗剰余演算回数は、2である。以上より、256ビットの素数を用いて、512ビットの素数を生成するために行う512ビットの冪乗剰余演算回数は、

$$(1 + 1/4) \times ((\ln \cdot 2^{512}) \times 8/35 - 1) + 2 = 89.5$$

以下である。

【0094】第1の実施の形態では、 $Lenq = 256$ ビットの素数から、 $2 \times Lenq = 512$ ビットの素数を生成するが、第1の実施の形態の素数生成部101を

\* $enq = 256$ ビットとし、 $2 \times Lenq = 512$ ビットの冪乗剰余演算における演算回数を見積もる。

【0090】一般に、数 $R$ を任意に選ぶ場合、 $R$ が素数となる確率は、 $1 / (\ln R)$ 程度であるので、この場合、512ビットの素数を生成するためにPocklington判定を試す回数は、 $\ln (2^{512})$ と見積もることができる。ここで、 $\ln R$ は、 $R$ の自然対数である。上記第1の実施の形態では、

$$N = 2 \times R \times q + 1$$

$$10 \quad = 2 \times L_1 \times L_2 \times \cdots \times L_n \times R' \times q + 1$$

であるので、

$$N = 1 \pmod{2},$$

$$N = 1 \pmod{L_1},$$

$$N = 1 \pmod{L_2},$$

$$\cdots, N = 1 \pmod{L_n} \text{ であり、} N \text{ は、} L_1, L_2, \cdots, L_n \text{ のいずれでも割り切れない。}$$

【0091】 $\pmod{2 \times L_1 \times L_2 \times \cdots \times L_n}$ の数が、2、 $L_1$ 、 $L_2$ 、 $\cdots$ 、 $L_n$ で割り切れない確率は、

$$20 \quad \phi(2 \times L_1 \times L_2 \times \cdots \times L_n) / (L_1 \times L_2 \times \cdots \times L_n) = (2-1) \times (L_1-1) \times (L_2-1) \times \cdots \times (L_n-1) / (2 \times L_1 \times L_2 \times \cdots \times L_n)$$

である。 $\phi$ は、オイラー関数と呼ばれ、辻井 重男、笠原 正雄、「暗号と情報セキュリティ」、昭晃堂、1990、11~12ページに詳しく説明されている。

【0092】従って、Pocklington判定を試す数の個数は、

$$(2-1) \times (L_1-1) \times (L_2-1) \times \cdots \times (L_n-1) / (2 \times L_1 \times L_2 \times \cdots \times L_n)$$

30 倍に削減できる。ここで、

$$L_1 = 3, L_2 = 5, L_3 = 7, n = 3 \text{ であるので、}$$

再帰的に使用することで、簡単に素数が分かる16ビットの素数から、512ビットの素数を生成することができる。よって、128ビットから256ビットの素数を生成する場合も同様に考えると、256ビットの素数を生成するために行う256ビットの冪乗剰余演算回数は、

$$(1 + 1/4) \times ((\ln \cdot 2^{256}) \times 8/35 - 1) + 2 = 45.1$$

以下である。

【0095】冪乗剰余演算の計算量は、法の $N$ に依存し、 $N$ の3乗のオーダーである。従って、256ビットの冪乗剰余演算8回を、512ビットの冪乗剰余演算1回相当と考えられる。64ビットから128ビットなどの他も同様に考えると第1の実施の形態の素数生成部101全体の計算量を、512ビットの冪乗剰余演算回数で

21

見積もることができる。16、32ビットの素数生成の計算量は、64、128、256、512ビットの素数生成の計算量に比べて小さいため無視し、第1の実施の形態1の素数生成部101全体の計算量を、512ビットの冪乗剰余演算回数で表すと、

$$(1+1/4) \{ ((1n \cdot 2^{64}) \times 8/35-1) / 512 + ((1n \cdot 2^{128}) \times 8/35-1) / 64 + ((1n \cdot 2^{256}) \times 8/35-1) / 8 + ((1n \cdot 2^{512}) \times 8/35-1) \} + 2(1/512 + 1/64 + 1/8 + 1) = 109.0$$

以下である。

【0096】これは、従来例1の116、8回以下と比べて、計算量が小さく、また、確定的に素数生成が可能になる。また、確定的な素数生成法である従来例2と比べて、2、2倍高速である。以上に説明したように、第1の実施の形態によると、従来例と比較すると、確定的な素数生成の計算時間を短縮できるという優れた効果がある。

【0097】しかしながら、第1の実施の形態によると、

$$N=1 \bmod 2、$$

$$N=1 \bmod L_1、$$

$$N=1 \bmod L_2、$$

… $N=1 \bmod L_n$  を満たす素数Nに限定して、素数生成を行うので、生成できる素数の種類が少ない。

【0098】暗号への使用を考えると、素数の種類が限定されることは、暗号の使用法によっては、安全性の面で懸念される場合がある。次に示す第2の実施の形態は、この問題を解決することを目的としている。

## 2. 第2の実施の形態

本発明に係る別の実施の形態としてのコンテンツ配信システム1b（図示していない）について、説明する。

【0099】コンテンツ配信システム1bは、コンテンツ配信システム1と同様に構成を有している。メモ리카ード10は、素数生成部101に代えて、素数生成部101bを備えている。ここでは、コンテンツ配信システム1との相違点を中心として説明する。

### 2.1 メモ리카ード10の生成制御部102

生成制御部102は、素数生成部101bへ、素数qと、素数qのビットサイズLenqと、2以外の小さな素数である $L_1、L_2、\dots、L_n$ と、 $(L_1 \times L_2 \times \dots \times L_n)$ のビットサイズLenLと、 $q \bmod L_1、q \bmod L_2、\dots、q \bmod L_n$ とを出力し、次に、素数生成部101bから1個の素数pを受け取り、受け取った素数pを素数paとして素数記憶部103へ書き込む。

【0100】次に、同様にして、素数生成部101bへ、素数qと、素数qのビットサイズLenqと、2以外の小さな素数である $L_1、L_2、\dots、L_n$ と、 $(L_1 \times L_2 \times \dots \times L_n)$ のビットサイズLenL、q m

22

od  $L_1、q \bmod L_2、\dots、q \bmod L_n$ とを出力し、次に、素数生成部101bから1個の素数pを受け取り、受け取った素数pを素数pbとして素数記憶部103へ書き込む。

【0101】2.2 メモ리카ード10の素数生成部101b

素数生成部101bは、素数q、 $q \bmod L_1、q \bmod L_2、\dots、q \bmod L_n$  ( $L_1、L_2、\dots、L_n$ は2以外の小さな素数)及び素数qのビットサイズLenqが与えられた場合、素数qのビットサイズの2倍のビットサイズをもつ素数pを生成して出力する。

【0102】ここで、 $L_1、L_2、\dots、L_n$ 及び $(L_1 \times L_2 \times \dots \times L_n)$ のビットサイズLenLは予め与えられているものとする。また、小さな素数の例として、入力される素数qのビットサイズより小さな素数が挙げられる。素数生成部101bは、図8に示すように、部分情報設定部136b、乱数生成部131b、判定対象生成部132b、第1素数判定部133b、第2素数判定部134b及び制御部135bから構成される。

【0103】(1) 部分情報設定部136b

部分情報設定部136bは、生成制御部102から素数q、 $q \bmod L_1、q \bmod L_2、\dots、q \bmod L_n$ を受け取り、 $2 \times u \times q + 1 \neq 0 \bmod L_1、2 \times u \times q + 1 \neq 0 \bmod L_2、\dots、2 \times u \times q + 1 \neq 0 \bmod L_n$

を満たす数uを算出し、算出した数uを判定対象生成部132bへ出力する。

【0104】部分情報設定部136bの詳細について以下に説明する。部分情報設定部136bは、図8に示すように、整数生成部141b及び情報合成部142bから構成される。

(整数生成部141b) 整数生成部141bは、乱数 $N_1$  ( $1 \leq N_1 \leq L_1 - 1$ )、 $N_2$  ( $1 \leq N_2 \leq L_2 - 1$ )、…、 $N_n$  ( $1 \leq N_n \leq L_n - 1$ )を発生し、 $u_i = (N_i - 1) / (2 \times (q \bmod L_i)) \bmod L_i$

( $i=1、2、\dots、n$ )

を計算する。

【0105】次に、計算して得た $u_i$  ( $i=1、2、\dots、n$ )を情報合成部142bへ出力する。

(情報合成部142b) 情報合成部142bは、整数生成部141bから $u_i$  ( $i=1、2、\dots、n$ )を受け取り、受け取った $u_i$  ( $i=1、2、\dots、n$ )を用いて、中国人の剰余定理から、

$$u = u_i \bmod L_i \quad (i=1、2、\dots、n)$$

を満たす $u \bmod (L_1 \times L_2 \times \dots \times L_n)$ を求める。

【0106】ここで、中国人の剰余定理については、岡本 栄司、「暗号理論入門」、共立出版、1993、10ページに詳しく述べられている。具体的には、情報合成部142bは、

$$\begin{aligned} u'_2 &= ((L_1)^{-1} \bmod L_2) \times ((u_2 - u_1) \bmod L_2) + u_1 \\ u'_3 &= ((L_1 \times L_2)^{-1} \bmod L_3) \times ((u_3 - u'_2) \bmod L_3) + u'_2 \\ \dots u'_n &= ((L_1 \times L_2 \times \dots \times L_{n-1})^{-1} \bmod L_n) \times ((u_n - u'_{n-1}) \bmod L_n) + u'_{n-1} \end{aligned}$$

を計算し、 $u = u'_n$  とする。

【0107】次に、情報合成部142bは、計算して得た数 $u$ を判定対象生成部132bへ出力する。(2) 乱数生成部131b

乱数生成部131bは、生成制御部102から $Len_q$ 及び $Len_L$ を受け取り、受け取った $Len_q$ 及び $Len_L$ を用いて、 $(Len_q - Len_L - 1)$ ビット長の乱数 $R'$ を生成し、生成した乱数 $R'$ を判定対象生成部132bへ出力する。

【0108】また、乱数生成部131bは、第1素数判定部133bから後述する第3判定情報を受け取る。また、第2素数判定部134bから後述する第4判定情報を受け取る。乱数生成部131bは、第3判定情報、又は第4判定情報を受け取ると、再度、受け取ったビットサイズ $Len_q$ 及び $Len_L$ を用いて、 $(Len_q - Len_L - 1)$ ビットサイズの乱数 $R'$ を生成し、生成した乱数 $R'$ を判定対象生成部132bへ出力する。

【0109】(3) 判定対象生成部132b  
判定対象生成部132bは、生成制御部102から素数 $q$ 、 $L_1$ 、 $L_2$ 、 $\dots$ 、 $L_n$ を受け取り、部分情報設定部136bから数 $u$ を受け取り、乱数生成部131bから乱数 $R'$ を受け取る。次に、受け取った素数 $q$ 、 $L_1$ 、 $L_2$ 、 $\dots$ 、 $L_n$ 、数 $u$ 及び乱数 $R'$ を用いて、以下の式を満たす数 $R$ 及び数 $N$ を生成する。

$$\begin{aligned} R &= u + L_1 \times L_2 \times \dots \times L_n \times R' \\ N &= 2 \times R \times q + 1 \end{aligned}$$

次に、判定対象生成部132bは、生成した数 $R$ 及び数 $N$ を第2素数判定部134bへ出力し、生成した数 $N$ を第1素数判定部133bへ出力する。(4) 第1素数判定部133b  
第1素数判定部133bは、判定対象生成部132bから数 $N$ を受け取り、受け取った数 $N$ を用いて、次の判定式3が成立するか否かを判定する。

【0111】 $2^{N-1} = 1 \bmod N$  (判定式3)  
判定式3が成立する場合には、第1素数判定部133bは、成立する旨を示す第3判定情報を第2素数判定部134bへ出力する。判定式3が成立しない場合には、成立しない旨を示す第3判定情報を乱数生成部131bへ出力する。

(5) 第2素数判定部134b

第2素数判定部134bは、判定対象生成部132bか

ら数 $R$ 及び数 $N$ を受け取る。また、第1素数判定部133bから判定式3が成立する旨を示す第3判定情報を受け取る。

【0112】第3判定情報を受け取ると、第2素数判定部134bは、受け取った数 $R$ 及び数 $N$ を用いて、次の判定式4が成立するか否かを判定する。

$$2^{2R} \neq 1 \bmod N \quad (\text{判定式4})$$

判定式4が成立する場合には、第2素数判定部134bは、数 $N$ を素数 $p$ として生成制御部102へ出力する。

【0113】判定式4が成立しない場合には、第2素数判定部134bは、判定式4が成立しない旨を示す第4判定情報を乱数生成部131bへ出力する。

(6) 制御部135b

制御部135bは、素数生成部101bを構成する各要素を制御する。

## 2. 3 素数生成部101bの検証

第1素数判定部133b及び第2素数判定部134bは、それぞれ素数生成部101bの第1素数判定部133及び第2素数判定部134と同じであるので、素数生成部101bは、素数生成部101と同様、素数を出力する。

【0114】また、乱数 $R'$ のビットサイズが $Len_q - Len_L - 1$ であるので、 $R$ のビットサイズが $Len_q - 1$ になり、 $N$ のビットサイズが $2 \times Len_q$ になる。

## 2. 4 素数生成部101bの動作

素数生成部101bの動作について図9に示すフローチャートを用いて説明する。

【0115】部分情報設定部136bは、 $2 \times u \times q + 1 \neq 0 \bmod (L_1 \times L_2 \times \dots \times L_n)$ を満たす $u$ を計算し、計算した $u$ を判定対象生成部132bへ出力する(ステップS152)。次に、乱数生成部131bは、 $Len_q - Len_L - 1$ ビットの乱数 $R'$ を生成し、生成した乱数 $R'$ を判定対象生成部132bへ出力する(ステップS153)。判定対象生成部132bは、 $R$ と $N$ を計算し、 $N$ を第1素数判定部133bへ出力し、 $N$ と $R$ を第2素数判定部134bへ出力する(ステップS154)。第1素数判定部133bは、判定式3の成立を判定し、成立しない場合は(ステップS155)、ステップS153へ戻って処理を繰り返す。

【0116】成立する場合は(ステップS155)、第2素数判定部134bは、判定式4の成立を判定し、成立しない場合は(ステップS156)、ステップS153へ戻って処理を繰り返す。成立する場合は(ステップS156)、第2素数判定部134bは、素数 $p$ として数 $N$ を生成制御部102へ出力し(ステップS157)、素数生成部101bは、処理を終了する。

## 【0117】2. 4 計算量の評価と効果

計算量については、第1の実施の形態とほぼ同じである。ただし、第1の実施の形態の計算量と比べて、部分



情報設定部136bの計算量のみが増加する。しかし、部分情報設定部136bは、 $\text{mod } L_1$ 、 $\text{mod } L_2$ 、 $\dots$ 、 $\text{mod } L_n$ の計算、及び中国人の剰余定理の計算のみであり、 $2 \times L \times n \times q$ ビットの数の計算と比較して、小さくほとんど0とみなしても問題ない。

【0118】従って、第2の実施の形態について、計算量に関し、第1の実施の形態と同等の効果が望める。また、 $N = N_1 \text{ mod } L_1$ 、 $N_2 \text{ mod } L_2$ 、 $\dots$ 、 $N_n \text{ mod } L_n$ であり、 $N_1$ 、 $N_2$ 、 $\dots$ 、 $N_n$ は乱数であるので、素数生成部101bは、生成する素数を限定しない。そのため、素数が限定されることによる安全性の懸念がなくなる。

【0119】従って、素数生成部101bによると、

(1) 生成する素数を限定しない、(2) 確定的な素数を生成する、(3) 従来例と比較して高速に素数を生成するという優れた効果がある。以上に説明したように第2の実施の形態によると、従来例と比較して、確定的な素数生成の計算時間を短縮でき、さらに、生成する素数の種類を限定しないため、素数を限定することによる安全性の懸念がなくなり、安全性の面でもよい。このことから、高速な暗号方式や署名方式を可能にする素数生成部を提供することができ、その実用的価値は大きい。

【0120】3. 変形例

第1の実施の形態、又は第2の実施の形態においてそれぞれ説明した素数生成を適用する暗号通信システム(図示していない)について説明する。暗号通信システムは、管理センタ装置、ユーザA装置及びユーザB装置から構成される。管理センタ装置、ユーザA装置及びユーザB装置は、それぞれ、相互にネットワークを介して接続されている。

【0121】管理センタ装置は、内部に、第1の実施の形態に示す生成制御部102及び素数生成部101を備え、生成制御部102及び素数生成部101により2個の素数 $p_a$ 及び素数 $p_b$ を生成する。なお、管理センタ装置は、内部に、第2の実施の形態に示す生成制御部102及び素数生成部101bを備えるとしてもよい。以下に、暗号通信システムの動作について、図10に示すフローチャートを用いて説明する。ここでは、素因数分解することが計算量上困難であることを安全性の根拠とするRSA暗号を応用している。RSA暗号については、岡本 龍明、山本 博資、「現代暗号」、産業図書、1997、110~113ページが詳しく説明されている。

【0122】(1) 管理センタ装置による公開鍵の生成  
管理センタ装置は、生成制御部102及び素数生成部101により、ランダムに素数 $p_a$ 及び素数 $p_b$ を生成し(ステップS171)、素数 $p_a$ 及び素数 $p_b$ を用いて、 $n = p_a \times p_b$ 、及び $L = \text{LCM}(p_a - 1, p_b - 1)$ を計算する(ステップS172)。

【0123】次に、管理センタ装置は、ランダムに乱数

$e$  ( $1 \leq e \leq L-1$ ,  $\text{GCD}(e, L) = 1$ )を発生させ、 $d = e^{-1} \text{ mod } L$ を計算する(ステップS173)。ここで、 $\text{GCD}(e, L)$ は、 $e$ と $L$ の最大公約数である。その後、管理センタ装置は、素数 $p_a$ 、素数 $p_b$ 及び数 $d$ を秘密鍵として、ユーザA装置に対して秘密裏に送信し(ステップS174)、ユーザB装置に対して、数 $n$ 及び数 $e$ をユーザA装置の公開鍵として公開して送信する(ステップS175)。

【0124】(2) ユーザB装置による暗号文の生成  
ユーザB装置は、 $c = m^e \text{ mod } n$ を計算する(ステップS176)。ここで、 $m$ は、ユーザB装置がユーザA装置へ送信するメッセージである。次に、ユーザB装置は、得られた $c$ を暗号文として、ユーザA装置に送信する(ステップS177)。

【0125】(3) ユーザA装置による暗号文の復号  
ユーザA装置は、 $m' = c^d \text{ mod } n$ を計算して、復号メッセージ $m'$ を得る(ステップS178)。ここで、

$$\begin{aligned} c^d &= (m^e)^d \text{ mod } n \\ &= m^{*} * (e \times d \text{ mod } L) \text{ mod } n \\ &= m^1 \text{ mod } n \\ &= m \text{ mod } n \end{aligned}$$

となることから、メッセージ $m$ が復号メッセージ $m'$ と同一であることは明らかである。

【0126】以上説明したように、公開鍵の生成のステップS171において、素数生成が行われる。この素数生成のステップにおいて、第1の実施の形態又は第2の実施の形態に示す生成制御部及び素数生成部が用いられるので、第1の実施の形態又は第2の実施の形態において説明した効果が得られる。

【0127】4. まとめ

以上説明したように、素数 $q$ と2以外の前記素数 $q$ より小さな素数 $L_1$ 、 $L_2$ 、 $\dots$ 、 $L_n$  ( $n \geq 2$ )とを入力とし、前記素数 $q$ より大きな素数 $N$ を出力する素数生成部は、素数 $q$ が、 $q = 1 \text{ mod } L_i$  ( $i = 1, 2, \dots, n$ )を満たし、 $N = 1 \text{ mod } L_i$  ( $i = 1, 2, \dots, n$ )を満たす $N$ を素数として生成する。

【0128】また、素数生成部は、乱数 $R'$ を生成し、前記素数 $q$ と前記乱数 $R'$ から、 $R = L_1 \times L_2 \times \dots \times L_n \times R'$ と、 $N = 2 \times R \times q + 1$ とを生成し、生成した前記 $N$ 及び前記 $R$ を用いて、前記 $N$ の素数判定を行う。また、素数 $q$ と2以外の前記素数 $q$ より小さな素数 $L_1$ 、 $L_2$ 、 $\dots$ 、 $L_n$  ( $n \geq 2$ )を入力とし、前記素数 $q$ より大きな素数 $N$ を出力する素数生成部は、 $2 \times u \times q + 1 \neq 0 \text{ mod } L_i$  ( $i = 1, 2, \dots, n$ )を満たす $u$ を出力し、乱数 $R'$ を生成し、生成した前記 $u$ 及び前記乱数 $R'$ を用いて、 $R = u + L_1 \times L_2 \times \dots \times L_n \times R'$ と、 $N = 2 \times R \times q + 1$ とを出力し、前記 $N$ 及び前記 $R$ を用いて、前記 $N$ の素数判定を行う。

【0129】また、前記素数生成部は、整数 $N_1$  ( $1 \leq$



$N_1 \leq L_1 - 1$ 、 $N_2$  ( $1 \leq N_2 \leq L_2 - 1$ )、 $\dots$ 、 $N_n$  ( $1 \leq N_n \leq L_n - 1$ ) を発生し、 $u_i = (N_i - 1) / (2 \times (q \bmod L_i)) \bmod L_i$  ( $i = 1, 2, \dots, n$ ) を計算し、前記  $u_i$  ( $i = 1, 2, \dots, n$ ) を用いて、 $u = u_i \bmod L_i$  ( $i = 1, 2, \dots, n$ ) を満たす  $u$  を計算する。

【0130】また、前記素数判定部は、前記  $N$  に対し、 $2^{N-1} = 1 \bmod N$  の成立を判定し、前記  $N$  及び  $R$  に対し、 $2^{2R} \neq 1 \bmod N$  の成立を判定する。このように、本発明によると、確定的な素数生成ができるとともに、従来例と比較して、計算時間を短縮できる。また、生成する素数の種類を限定しないようにできるので、素数を限定することによる安全性の懸念がなくなり、安全性の面でもよい。

【0131】以上により、高速な暗号方式や署名方式を可能にする情報セキュリティ装置及び素数生成装置を提供することができ、その実用的価値は大きい。

#### 5. その他の変形例

以上、実施の形態に基づいて説明したが、本発明はこれらの実施の形態に限られないことは勿論である。次のように構成してもよい。

【0132】(1) 本発明は、本実施の形態に示す素数生成部により、整数  $Len$  を入力とし、 $Len$  ビットの素数を出力するとしてもよい。

(2) 上記において説明した素数生成部は、独立した 1 個の装置であるとしてもよい。

(3) 本発明は、本実施の形態に示す素数生成部を備える素数応用装置であるとしてもよい。素数応用装置の具体的な例は、暗号化装置及び暗号復号装置からなる暗号通信システム、デジタル署名作成装置及び署名検証装置からなるデジタル署名システムである。これらのシステムは、情報を安全かつ確実に扱う情報セキュリティシステムである。

【0133】(4) 第 1 素数判定部 133、第 2 素数判定部 134、第 1 素数判定部 133b、第 2 素数判定部 134b は、上記実施の形態と異なる素数判定式を使用するとしてもよい。例えば、第 1 素数判定部 133 及び第 1 素数判定部 133b は、次の判定式を用いるとしてもよい。

【0134】 $a^{N-1} = 1 \bmod N$

としてもよい。但し、 $a$  は  $1 \leq a \leq N-1$  を満たす整数である。また、第 2 素数判定部 134 及び第 2 素数判定部 134b は、つぎの判定式を用いるとしてもよい。

$b^{2R} \neq 1 \bmod N$

又は、

$GCD(b^{2R} - 1, N) = 1$

としてもよい。但し、 $b$  は  $1 \leq b \leq N-1$  を満たす整数である。

【0135】(5) デジタル著作物は、音楽であるとしているが、その他のデジタル情報であるとしてもよい。

例えば、音声、動画像、静止画像、文章、表形式のデータ、コンピュータプログラムなどのデジタル情報であるとしてもよい。

(6) 上記の実施の形態において、RSA 暗号を適用するセキュリティシステムにおける素数生成部について説明しているが、素数生成部の利用は、RSA 暗号を適用するセキュリティシステムに限定されるものではない。例えば、楕円暗号において、素数生成部を適用することが可能である。楕円暗号では、1 個の素数を生成して用いる。

【0136】(7) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【0137】また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【0138】また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(7) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

#### 【0139】

【発明の効果】上記目的を達成するために、素因数分解をすることが計算量の上で困難であることを根拠として、2 個の素数を生成し生成した 2 個の素数の乗算を用いて、所定の情報を安全かつ確実に扱い、各素数生成の際に、既知の素数  $q$  の 2 倍のビット長を有する素数  $N$  を生成する情報セキュリティ装置であって、素数  $q$  及び  $n$  個の素数  $L_1$ 、 $L_2$ 、 $\dots$ 、 $L_n$  を取得し、ここで、素数  $L_1$ 、 $L_2$ 、 $\dots$ 、 $L_n$  は、それぞれ素数  $q$  より小さい 2 以外の素数であり、素数  $q$  は、 $q = 1 \bmod L_i$  ( $i = 1, 2, \dots, n$ ) を満たす取得手段と、取得した前記素数  $L_1$ 、 $L_2$ 、 $\dots$ 、 $L_n$  に係る

数を除外した選択により、取得した前記素数 $q$ の2倍のビット長を有する数 $N$ を生成する生成手段と、生成した数 $N$ の素数判定を行い、数 $N$ が素数であると判定とされた場合に、数 $N$ を素数として出力する判定手段とを備える。

【0140】この構成によると、確定的な素数生成ができるとともに、従来と比較して、計算時間を短縮できる。また、前記生成手段は、 $N=1 \bmod L_i$  ( $i=1, 2, \dots, n$ ) を満たす前記数 $N$ を生成する。また、前記生成手段は、 $(Len_q - Len_L - 1)$  ビット長の乱数 $R'$ を生成し、ここで、 $Len_q$ は、素数 $q$ のビット長であり、 $Len_L$ は、 $(L_1 \times L_2 \times \dots \times L_n)$  のビット長である乱数生成部と、生成した $R'$ 及び前記素数 $L_1, L_2, \dots, L_n$ を用いて、数 $R=L_1 \times L_2 \times \dots \times L_n \times R'$ により、数 $R$ を生成し、取得した素数 $q$ 及び生成した数 $R$ を用いて、数 $N=2 \times R \times q + 1$ を生成する判定対象生成部とを含み、前記判定手段は、前記数 $N$ 及び前記数 $R$ を用いて、前記数 $N$ の素数判定を行う。

【0141】この構成によると、計算時間を短縮できる。また、前記生成手段は、取得した前記素数 $q$ を用いて、 $2 \times u \times q + 1 \neq 0 \bmod L_i$  ( $i=1, 2, \dots, n$ ) を満たす数 $u$ を生成する部分情報生成部と、乱数 $R'$ を生成する乱数生成部と、取得した前記素数 $L_1, L_2, \dots, L_n$ と、生成した前記数 $u$ と、生成した前記乱数 $R'$ を用いて、 $R=u + L_1 \times L_2 \times \dots \times L_n \times R'$ により、数 $R$ を生成し、取得した前記素数 $q$ と、生成した数 $R$ とを用いて、 $N=2 \times R \times q + 1$ により、数 $N$ を生成する判定対象生成部とを含み、前記判定手段は、前記数 $N$ 及び前記数 $R$ を用いて、前記数 $N$ の素数判定を行う。

【0142】この構成によると、生成する素数の種類を限定することなく、計算時間を短縮できる。

#### 【図面の簡単な説明】

【図1】コンテンツ配信システム1の構成を示すブロック図である。

【図2】メモリカード10の構成を示すブロック図である。

【図3】素数生成部101の構成を示すブロック図である。

【図4】PC30の構成を示すブロック図である。

【図5】配信サーバ装置40の構成を示すブロック図で

ある。

【図6】コンテンツ配信システム1の動作を示すフローチャートである。

【図7】素数生成部101の動作を示すフローチャートである。

【図8】素数生成部101bの構成を示すブロック図である。

【図9】素数生成部101bの動作を示すフローチャートである。

【図10】暗号通信システムの動作を示すフローチャートである。

#### 【符号の説明】

1 コンテンツ配信システム

10 メモリカード

20 PDA

21 ヘッドフォン

30 PC

40 配信サーバ装置

50 携帯電話

60 インターネット

61 無線基地局

62 携帯電話網

101 素数生成部

102 生成制御部

103 素数記憶部

104 乱数生成部

105 秘密鍵記憶部

106 公開鍵生成部

107 公開鍵記憶部

108 復号部

109 メモリ部

110 セキュア領域

111 一般領域

112 制御部

113 認証部

114 送受信部

131 乱数生成部

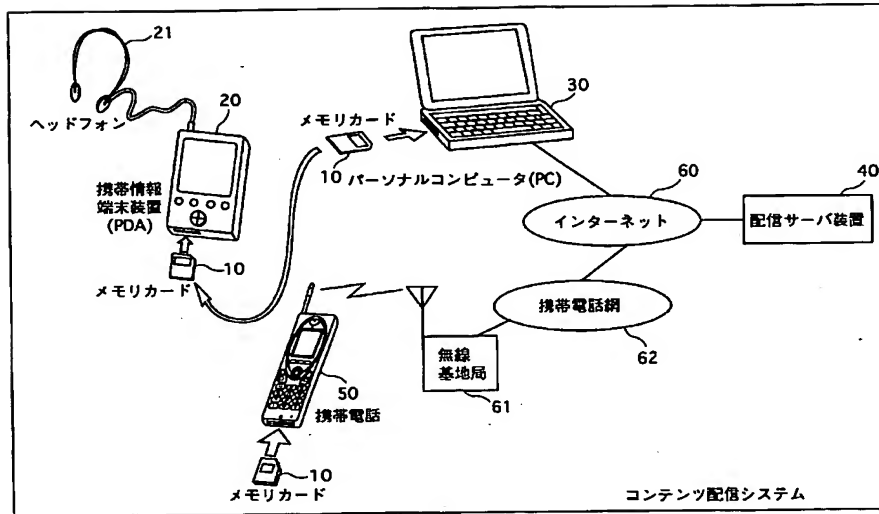
132 判定対象生成部

133 第1素数判定部

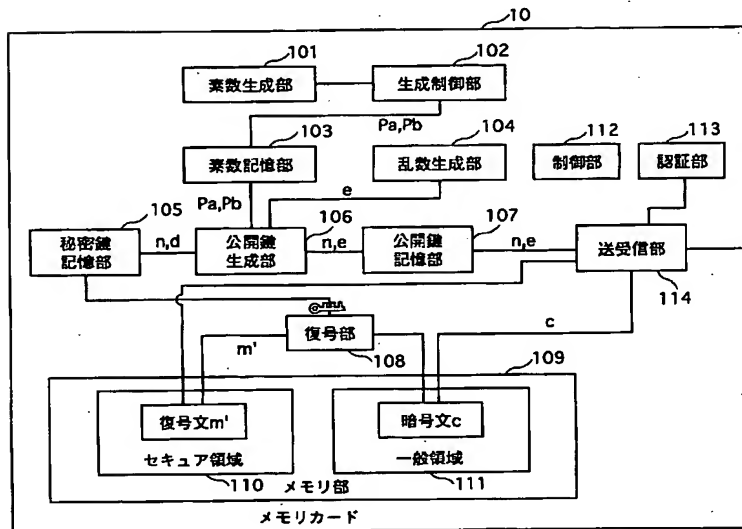
134 第2素数判定部

制御部

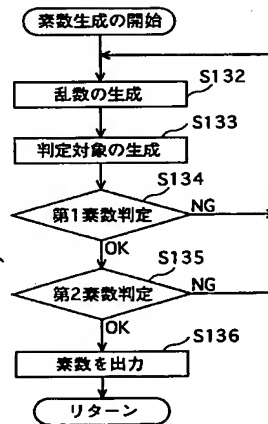
【図1】



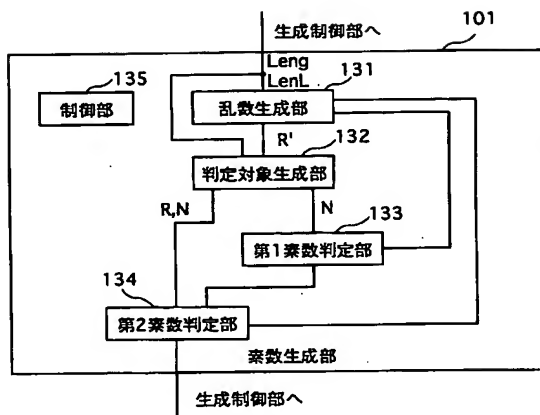
【図2】



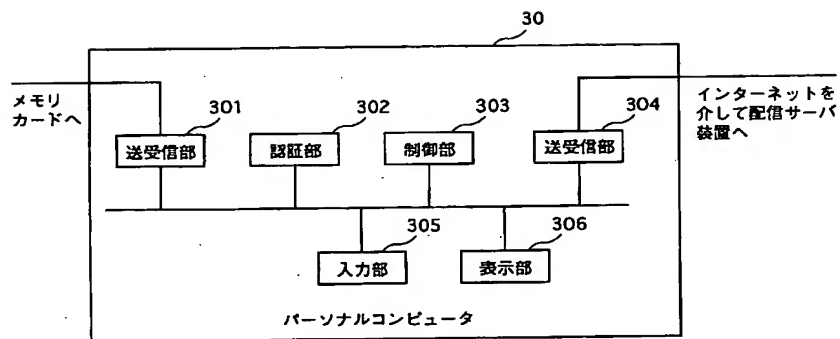
【図7】



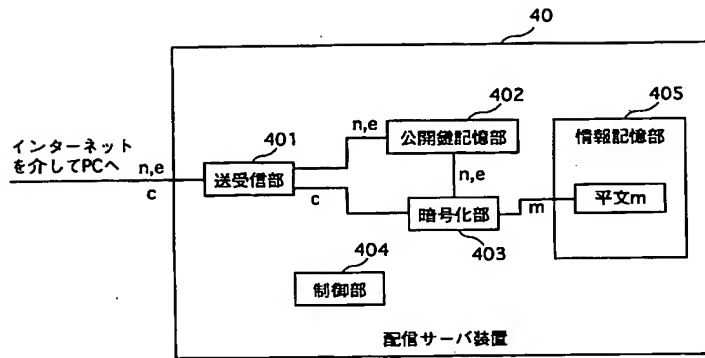
【図3】



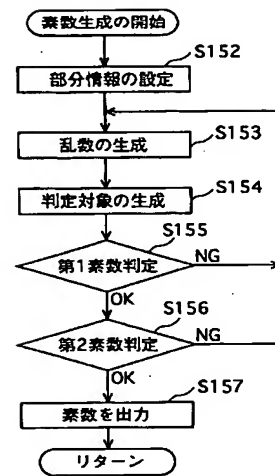
【図4】



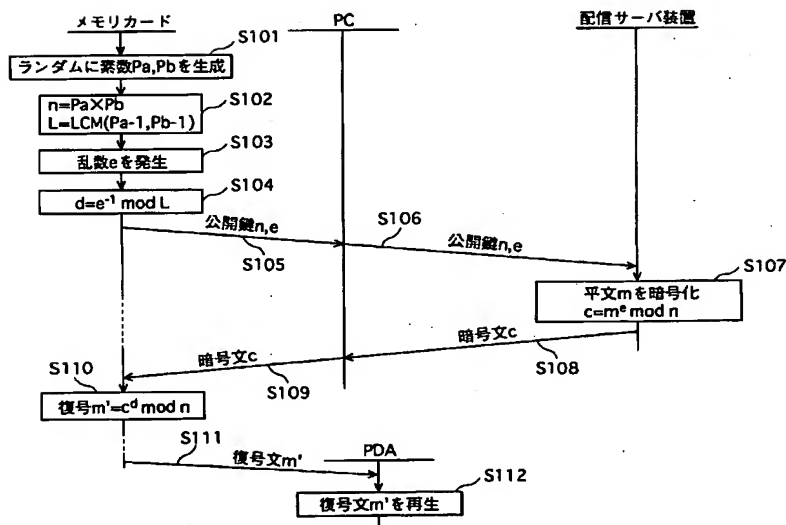
【図5】



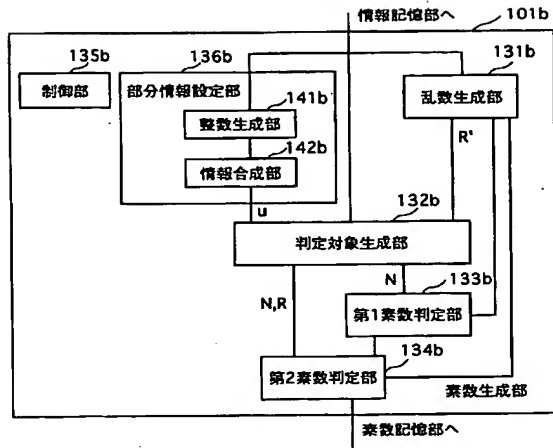
【図9】



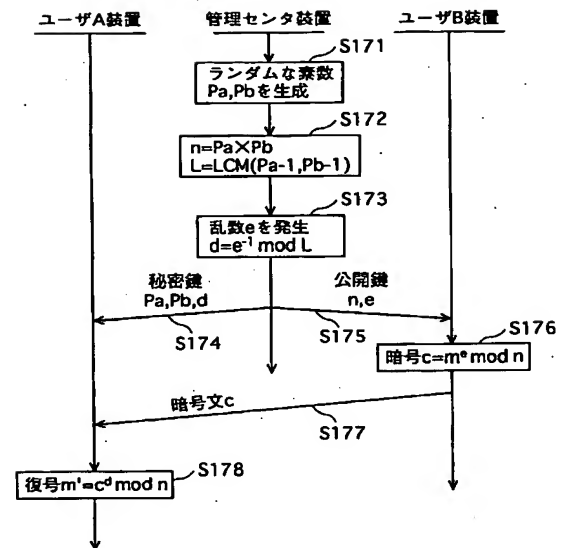
【図6】



【図8】



【図10】



フロントページの続き

(72) 発明者 大森 基司  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

Fターム(参考) 5J104 AA23 EA04 EA19 EA32 JA28  
NA02 NA18 NA35